REBECCA HYDE SKORDAS (6409)
Skordas, Caston, & Hyde
341 S. Main Street, Suite 303
Salt Lake City UT 84111-2707
Telephone: (801) 531-74444
Facsimile: (801) 531-8885

Daniel Marino (admitted *pro hac vice*)
Tillman J. Finley (admitted *pro hac vice*)
MARINO LAW PLLC
910 17th Street, N.W., Suite 800
Washington, DC 20006
Telephone: (202) 223-8888
Facsimile: (877) 239-2146

Attorneys for Michael Taylor

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH
CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ROBERT G. LUSTYIK, JR., *et al.*, Defendants.	Case No. 2:12-CR-00645 Judge Tena Campbell

MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS

Defendant Michael Taylor moves to suppress all evidence seized by the government purportedly pursuant to search warrants obtained through the use of evidence seized in violation of the Fourth Amendment in connection with the investigation and prosecution of the *United States v. Young* case, No. 2:12-cr-502, specifically email communications and other documents relating to communications between Mr. Taylor and Special Agent Lustyik and/or Defendant Thaler As detailed *infra*, this includes all evidence obtained pursuant to not only the seven

search warrants directed at email accounts and/or property allegedly associated with Mr. Taylor, but also numerous other warrants directed at the property of Special Agent Lustyik and Defendant Thaler. All of these warrants were obtained through the use of evidence seized in violation of Mr. Taylor's constitutional rights and, therefore, are subject to suppression as fruit of the poisonous tree.

Further, even if they were not fruit of the poisonous tree, each of the seven search warrants directed at Mr. Taylor's email accounts and/or property (and issued on June 13, 2012; August 2, 2012; September 7, 2012; September 21, 2012; October 18, 2012; and January 1, 2013—*see* Exhibits A-G) is invalid on its face in that it purports to sanction an unconstitutional general search in the form of a wholesale seizure of the entirety of the content of certain email accounts, computers, and devices to be subjected to wide-ranging, leisurely rummaging by the investigators and prosecutors over the course of the case. Even if, however, the terms of the warrants could be construed so favorably to the government as to render them arguably valid, the searches conducted under their auspices in fact constituted unconstitutional general searches and the resulting seizures are subject to suppression.

FACTUAL AND PROCEDURAL BACKGROUND

As detailed in Defendants Taylor and AISC's Motion to Suppress in the *Young* case, in December 2011, the government obtained three search warrants directed at an email account associated with Mr. Taylor and various computers and computer systems belonging to Mr. Taylor and/or his company, AISC. Those warrants, however, purported to authorize a general search of the entire contents of these materials and that is exactly what the government proceeded to do over the course of the following months and years. In April 2012, in the course of this general rummaging through the electronic data, a contractor hired by the government to

sift through the email and other electronic documents stumbled across an email containing derogatory references to the lead investigator, DCIS Special Agent Keith Darnell. She sent the email to SA Darnell "to rile [him] up" telling him that some guy with the email address "blustyik" was "badmouthing" him. SA Darnell proceeded to review the email and, even though he admittedly "disregarded it," he nevertheless (and without seeking a new warrant) asked for and proceeded to review all emails relating to the email address. (*See Young*, Doc. No. 332 at 18-19.) This general rummaging through Mr. Taylor's computer and email account resulted in the generation of a report of communications between Ms. Auterio and/or Mr. Taylor and Special Agent Lustyik and the assembly of 272 pages of emails from 2011 involving Johannes Thaler and FBI Special Agent Robert Lustyik.

That information was then handed over to the lead investigator in this case, Special Agent Thomas M. Hopkins of the Department of Justice's Office of the Inspector General (DOD-OIG). SA Hopkins proceeded to peruse the emails himself, searching even more generally for contacts and communications with employees or contractors of the CIA, FBI, and other intelligence agencies. (*See, e.g.*, Exh. H.) The *Lustyik* investigators then used this information to seek additional search warrants directed at various email accounts, mobile telephone devices, computers, residences, and offices.

As specific to Mr. Taylor's property, seven additional warrants were obtained. First, on June 13, 2012, the government sought a new search warrant directed at the aisc01@aol.com email account (Exh. A) with further such warrants directed at the same email account on September 7, 2012 and January 15, 2013. (Exhs. C & G.) The June 13 warrant was issued by Magistrate Judge Samuel Alba; the September 7 warrant was issued by Magistrate Judge Dustin Pead; and the January 15 warrant was issued by Magistrate Judge Evelyn J. Furse. In addition,

on August 2, 2012, the government obtained a search warrant directed at two other email accounts purportedly used by Mr. Taylor, aisc04@aol.com and bme2012@aol.com. (Exh. B.) That warrant was issued by Magistrate Judge Furse. The foregoing are hereinafter referred to collectively as "the AOL Warrants" and individually by reference to their date.

The applications for the first three AOL Warrants were supported by an affidavit executed by SA Hopkins (Exhs. I, J, & K.) The application for the January 15, 2013 AOL Warrant was supported by an affidavit executed by DOJ-OIG Special Agent Kerwin John. (Exh. O.) All four AOL Warrants have an Attachment B which employs substantially identical language requiring AOL to provide the government with copies of "[a]ll data files associated with the e-mail address or account" and "[a]ll subscriber and transaction records for the … e-mail account and any associated e-mail accounts and secondary contact e-mail accounts" and call for the government to then seize from such copies "[e]vidence, fruits, or instrumentalities of" certain specified violations. The June 13, 2012 AOL Warrant referred to "violation of 18 U.S.C. § 1503(a) (Influencing or Injuring Officer or Juror Generally involving Robert Lustyik or Michael Taylor since January 1, 2009" (Exh. A); the August 2 and September 7, 2012 AOL Warrants refer to "violation of 18 U.S.C. § 1503(a) (Influencing or Injuring Officer or Juror Generally), 208 (Acts Affecting Personal Financial Interest), 1341, 1343, and 1346 (Honest Services Mail and Wire Fraud) involving Robert Lustyik or Michael Taylor since January 1, 2009" (Exhs. B & C); and the January 15, 2013 AOL Warrant simply refers to "the violations charged in the Indictment in United States v. Robert Lustyik, Jr., et al., 2:12-cr-645-TC, during the time period of the conspiracy charged within that Indictment (October 2011 to September 2012)." (Exh. G.)

Each AOL warrant follows the identification of the supposed violations with the

following language:

A. …, including, ***without limitation***, information relating to:

1. All communications between or among Robert Lustyik, Michael Taylor, including Taylor's business e-mail addresses;

2. All records pertaining to any business relationship between or among Robert Lustyik, Michael Taylor, and Johannes "Hannes" Thaler;

3. All records or communications consisting of or pertaining to Robert Lustyik's contact with Michael Taylor's business or business associates, including Johannes "Hannes" Thaler;

4. All records or communications consisting of or pertaining to Robert Lustyik's contact with individuals concerning the investigation of Michael Taylor and/or AISC;

5. All records or communications pertaining to Michael Taylor providing Robert Lustyik or Johannes "Hannes" Thaler with anything of value;

6. The identity of the person or persons who have owned or operated the … email account or any associated email accounts;

7. The existence and identity of any co-conspirators;

8. The travel or whereabouts of the person or persons who have owned or operated the … e-mail account or any associated e-mail accounts;

9. The identity, location, and ownership of any computers used to access this e-mail account;

10. Other e-mail or Internet accounts providing Internet access or remote data storage for Taylor or any associated e-mail accounts; and

11. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber and transaction records described in Sections II(B).

(Exhs. A, B, C, & G (emphasis added).)

The government also obtained three other warrants directed at telephone and computer

devices seized from Mr. Taylor. Specifically, on September 21, 2012 they obtained a warrant from Magistrate Judge John M. Facciola of the District Court for the District of Columbia to search a mobile telephone device seized from Mr. Taylor at the time of his arrest (Exh. D) and, on October 18, 2012, they obtained two warrants from Magistrate Judge Leo T. Sorokin of the District of Massachusetts, directed at images of another mobile telephone device and laptop computer, respectively, seized from Mr. Taylor upon his return to the country on September 8, 2012 to appear at his arraignment in the *Young* case (Exhs. E & F.) Attachment B to the September 21 phone warrant is substantially identical to the Attachment B that accompanied the August 2 and September 7, 2012 AOL Warrants except that it excludes the last three items from the "including, without limitation" list. Attachment B to both of the October 18 warrants is the same, except that it adds Michael Feldman[1] to the list of persons or business associates listed in the second and third items of the "including, without limitation" list and revises the referenced violations to include "18 U.S.C. § 371 (Conspiracy)" and "18 U.S.C. § 1505 (Obstruction of Proceeding before Department or Agency)" and to omit references to the mail fraud statute and § 208 (Acts Affecting a Personal Financial Interest).

ARGUMENT

The Fourth Amendment provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const., amend. IV. "The Amendment is to be liberally construed and all owe the duty of vigilance for its effective enforcement lest there shall be impairment of the rights for the

[1] Albeit without any explanation in the search warrant affidavit for who this person is or why probable cause exists to seized any communications with or relating to him. These warrants, therefore, exceed the scope of whatever probable cause might be stated by the affidavit in any event.

protection of which it was adopted." *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931).

The Fourth Amendment's Warrants Clause was intended as a bulwark against "the 'general warrant' abhorred by the colonists" and protects against "a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999) ("It is axiomatic that the 4th Amendment was adopted as a direct response to the evils of the general warrants in England and the writs of assistance in the Colonies."). Its overarching purpose is to ensure that "those searches deemed necessary should be as limited as possible." *Coolidge*, 403 U.S. at 467; *see also United States v. Foster*, 100 F.3d 846, 849 n.3 (10th Cir. 1996).

To achieve this goal, the Fourth Amendment requires particularity and forbids overbreadth. "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993) (quotations omitted). "The manifest purpose of [the] particularity requirement was to prevent general searches. By limiting the authorization to search the specific areas …, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). "The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." *United States v. Otero*, 563 F.3d 1127,

1132 (10th Cir. 2009).

Thus, a warrant can violate the Fourth Amendment by seeking specific material as to which no probable cause exists, by seeking a group or class of material broader than that for which probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries. Government agents may only seize items that are described in the warrant, and "nothing is [to be] left to the discretion of the officer …." *Foster*, 100 F.3d at 849; *see also United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) ("As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized."). A general warrant is one that so clearly violates the particularity requirement that it "vest[s] the executing officers with unbridled discretion to conduct an exploratory rummaging through [defendants'] papers in search of criminal evidence." *United States v. Christine*, 687 F.2d 749, 753 (3d Cir. 1982). "It is beyond doubt that all evidence seized pursuant to a general warrant must be suppressed." *Id.* at 758.

With these general principles in mind, we examine the various warrants, searches, and seizures in these cases.

I. Evidence of Communications between Mr. Taylor, Special Agent Lustyik, and Mr. Thaler Unlawfully Seized in Connection with the *Young* Case Must Likewise Be Suppressed in the *Lustyik* Case

As detailed *supra* and in the Motion to Suppress filed in the *Young* case (which is incorporated herein by reference), the government unlawfully seized a number of 2011 emails between Mr. Taylor, Special Agent Lustyik, and/or Mr. Thaler under the auspices of unconstitutionally broad December 2011 search warrants and in blatant disregard of the notion that their perusal of the entire contents of Mr. Taylor and AISC's email and computers was subject to any sort of limitation. The government has produced as discovery in this case two collections of emails seized in the *Young* case, specifically "Emails between R. Lustyik and M.

Taylor retrieved during search warrant obtained and executed by prosecution team in *U.S. v. Young*, 2:12-cr-502-TC, of the email address aisc01@aol.com" (Bates numbers US00170627-00170815) and "Emails between R. Lustyik and M. Taylor retrieved during search warrant obtained and executed by prosecution team in *U.S. v. Young*, 2:12-cr-502-TC, of electronic media belonging to Mr. Taylor" (Bates numbers.US00170876-00170889). These emails were not, and could not have been, lawfully seized under the December 2011 warrants and that should be suppressed in this case for the same reasons they should be suppressed in *Young*.

II. All of the *Lustyik* Search Warrants Are Fruit of the Poisonous Tree

The government, of course, does not merely wish to use the emails unlawfully seized in the *Young* case as evidence at trial. It already has made substantial use of them in its investigation, including to justify additional search warrants, fatally tainting all of those efforts. The NTI contractor's April 2012 teasing email to SA Darnell commenting upon a 2011 email she had found between Mr. Taylor and Special Agent Lustyik and SA Darnell's subsequent seizure and review of all emails involving the same address without obtaining a new warrant set in motion SA Hopkins' analysis and investigation and, ultimately, his actions in seeking search warrants for the email of Special Agent Lustyik, Mr. Thaler, and Mr. Taylor in May and June 2012, all of which were based in substantial part on the unlawfully-seized emails.

SA Hopkins' affidavit in support of the June 13, 2012 AOL Warrant stated that the government now was investigating FBI Special Agent Robert Lustyik, Jr. "for attempting to influence the investigation by federal law enforcement officers and prosecutors in the District of Utah of allegations of theft of federal funds, wire fraud and money laundering involving Michael Taylor, an individual with whom Lustyik has a personal business relationships, in violation of 18 U.S.C. § 1503(a) (Influencing or Injuring Officer or Juror Generally)." (Exh. I ¶ 2.) Central to

SA Hopkins' claim of probable cause to support the search of Mr. Taylor's emails was the allegation that Mr. Taylor had a "personal business relationship" with Agent Lustyik (*id.* ¶ 2) and that he used the email account aisc01@aol.com "to communicate with an e-mail account operated by Lustyik, regarding mutual business activities between the two and others, as well as to communicate concerning the federal investigation of which Taylor is a target" (*id.* ¶ 3).[2]

To support those allegations, SA Hopkins relied upon "emails [that] were obtained through a search warrant of Taylor's e-mails in the Utah criminal investigation" to establish "that Taylor communicates with Lustyik via e-mail." (*Id.* ¶ 10.) He stated that "[t]he USAO investigation of Taylor identified approximately 70 e-mail messages made between Taylor's e-mail account and blustyik16@hotmail.com from approximately June 2011 through approximately December 2011." (*Id.* ¶ 43.) The affidavit proceeds to discuss and quote from those emails, and to draw conclusions therefrom (*see id.* ¶¶ 11-20, 40-50.), including "that the two are involved in a business relationship involving, among other things, the procurement of business for Taylor in South Sudan" (*id.* ¶ 12), that blustyik16@hotmail.com is even Mr. Lustyik's email address to begin with (¶¶ 41-44), and that they "discussed the Utah criminal investigation" (¶ 45-47), and that "Lustyik had been dealing with Taylor since at least June 2011" (¶ 48).

SA Hopkins used the same unlawfully-seized emails in the same fashion in his affidavits in support of the May 23, 2012 search warrant directed at the email address blustyik16@hotmail.com (*see* Exh. P ¶¶ 3, 11-17, 32-35, 37-42) and a June 13, 2012 warrant

[2] SA Hopkins' affidavit also gratuitously misstates and overstates the wrongdoing by Mr. Taylor alleged in the *Young* case, claiming that the allegations against Mr. Taylor "include (1) that Taylor bribed *several* DoD officials …; (2) that Taylor committed conspiracy *to defraud DoD* in connection with procuring the contract; (3) that Taylor's company, AISC, *submitted false claims for payments from the contract*; and (4) that individuals associated with the scheme, *including Taylor*, thereafter engaged in money laundering …." (Exh. I ¶ 8 (emphasis added).) As the Court is aware, the italicized components of the foregoing statements are not part of the allegations against Mr. Taylor in the *Young* case and the government has no evidence whatsoever to support those assertions.

directed at the email address hannestee@yahoo.com (*see* Exh. Q ¶¶ 3, 10-11, 13-25, 45, 47-53).

Because these emails were unlawfully seized by the government in the course of its investigation of the 2007 procurement of AISC's contract with the U.S. Army for training work in Afghanistan, their use in SA Hopkins' search warrant affidavits violates the Fourth Amendment. "Under the fruit of the poisonous tree doctrine, the exclusionary rule bars the admission of physical evidence and live testimony obtained directly or indirectly through the exploitation of unconstitutional police conduct." *United States v. Hatfield*, 333 F.3d 1189, 1193-94 (10th Cir. 2003) (citing *Wong Sun v. United States*, 371 U.S. 471, 485-88 (1963)). If police "conduct [ ] unconstitutional searches that acquire[ ] information used to obtain [a] search warrant," then "evidence seized during the later search conducted pursuant to warrant would be inadmissible as fruit of the poisonous tree." *Id.* at 1194.

This is precisely what happened here. The initial unconstitutional seizures by the *Young* investigators were taken and used by the *Lustyik* investigators to obtain the series of search warrants in this case. Without the nexus between Mr. Taylor and Lustyik, the affidavits fail to establish probable cause to search Mr. Taylor's, Lustyik's, or Thaler's emails for evidence of Lustyik's alleged wrongdoing. Accordingly, the May 23, 2012 Microsoft search warrant, the June 13, 2012 AOL search warrant, and the June 13, 2012 Yahoo search warrant all are fruit of the poisonous tree and all evidence obtained as a result of those warrants must be suppressed.[3]

The government did not stop there though. It proceeded to use the emails seized in the *Young* case and the information seized pursuant to the initial round of tainted email warrants in

[3] Specifically, the materials directly seized pursuant to these warrants are as follows: Taylor-AOL Warrant (US00000001-00075052, US00092929-00093841, US00103246-00118070, US00130880-00137989, US00137993-00138264, US01070628-01073868); Lustyik-Microsoft Warrant (US00077011-00083349, US00093971-00094084, US00118071-00118111, US00154228-00154233, US00154235-00154239, US01076167-01076271); and Thaler-Yahoo Warrant (US00083350-00092927, US00094282-00094495, US00118112-00121254, US01092081-01092097).

the *Lustyik* case to obtain additional, follow-up email warrants[4] and to obtain warrants for other searches. Specifically, in addition to the aforementioned warrants for searches of mobile telephones and a laptop seized from Mr. Taylor, the government used the same emails from the *Young* case in September 17, 2012 applications for warrants to search Lustyik's Blackberry device and home used (Exhs. R & S ¶¶ 13-19, 22, 42-46, 53, 60-61) and along with the tainted evidence obtained through the initial round of *Lustyik* email warrants (*id.* ¶¶ 20-21, 47-53, 55, 60-61). As did September 14, 2012 applications for warrants to search Mr. Thaler's home and iPhone device. (*See* Exh. T ¶¶ 16-17, 19-24, 45-51, 54-55.) The government proceeded in the same fashion to obtain further warrants, including ones directed at Special Agent Lustyik's work space and his text messages and one directed at computer hard drives belonging to Mr. Thaler.

A hearing is necessary to explore the full scope and extent of the government use, both direct and indirect, of the evidence unlawfully-seized in the *Young* case. At a minimum, however, all of the evidence seized under the previously-referenced search warrants must be suppressed as fruit of the poisonous tree.[5]

---

[4] In addition to the August, 2, 2012, September 7, 2012, and January 15, 2013 AOL Warrants identified previously, the government used the same tainted information to obtain August 2, 2012 and January 15, 2013 warrants directed at the email address blustyik16@hotmail.com, and a September 7, 2012 warrant directed at the email address hannestee@yahoo.com.

[5] Specifically, Aug. 2, 2012 AOL Warrant (US00075053-00077010); Aug. 2, 2012 Microsoft Warrant (US00154234); September 7, 2012 AOL Warrant (US00137990-00137992, US00138265-00139606); Sept. 7, 2012 Yahoo Warrant (US00094485-00094487, US00170890-00170910, US00170989-00171019, US00171066-00171402); Sept. 21, 2012 Taylor phone warrant (US00130174-00130248, US00170572-00170618); Oct. 18, 2012 Taylor phone and laptop warrants (US00130381-00130388, US00130845-00130865, US00171403-00274781, US00998063-01064327, US01069669-01070295, US01076746-01091303); Thaler home (US00122879-00127729, US00130795-00130825, US01069663-01069668, US01073938-01073969); Thaler iPhone (US00094124-00094246, US00130128-00130149, US00130249-00130280, US00154848-00157097, US00157408-00158252, US00158263-00158297, US00159279-00159282, US01073984, US01076666-01076669, US01091323-01091734); Thaler hard drives (US00130640-00130656, US00274782-00998062, US01089066-01091126); Lustyik home (US00121735-00122878, US00130409-00130422, US00130626-00130639, US01091757-01091761, US01091770-01091812); Lustyik Blackberry (US00130297-00130313, US00157407, US00159283-00159290, USDOJPROD007, US01075291-01075293); Lustyik office (US00130688-00130743, US01069507-01069632, US01091762-01091769, US01091813-01091990); Dec. 5, 2012 Lustyik Text Messages (US00158337-00159278); Jan. 15, 2013 Microsoft Warrant (US0015420-00154320, US00154323-00154336), Jan. 15, 2013 AOL Warrant (US00139607-00148752).

III. The Warrants Are Facially Invalid General Searches

Even if not the products of evidence previously seized unlawfully, all seven *Lustyik* warrants directed at Mr. Taylor's property are themselves facially invalid as unconstitutional general searches. Each of the warrants purports to authorize the government to seize "evidence, fruits, or instrumentalities" of a shifting list of anywhere from one (June 13, 2012 AOL Warrant) to five (the other five warrants) statutory offenses. The language thus restricts the scope of the search and seizures only by reference to a criminal statute(s), the violation of which supposedly is being investigated.

"An unadorned reference to a broad federal statute does not sufficiently limit the scope of a search warrant." *United States v. Leary*, 846 F.2d 592, 602 (10th Cir. 1988).). The warrant's description of the items to be seized must "describe the items to be seized with as much specificity as the government's knowledge and circumstances allow," *id.* at 600, and they must provide some clear limitation on the scope of the search. "As an irreducible minimum, a proper warrant must allow the executing officers to distinguish between items that may and may not be seized." *Id.* at 602. "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927).

The list of 8 to 11 items provided in each of the Attachments B cannot save the warrants because the Attachment itself specifically disclaims any limitation that might be suggested by the list. Each list is expressly set off with the language "including, ***without limitation***, information relating to …." (Exhs. A-G (emphasis added).) Because the operative language of the Attachment expressly disclaims any notion of exclusivity, the list provides no meaningful limitation on the scope of the warrant. *Cf. United States v. Fleet Mgm't Ltd.*, 521 F. Supp. 2d 436, 443 (E.D. Pa. 2007) (holding warrant authorizing computer search for "any and all data

from the three seized computers, *including, but not limited to* certain types of data relating to the Ship's operation, engineering, maintenance, pollution control equipment, navigational charts, and crew" did not place any restrictions on search) (emphasis added).

In *Leary*, *supra*, a search warrant purported to authorize the search of a company's offices and the seizure of a list of categories of business records "and communications relating to the purchase, sale and illegal exportation of materials in violation of the Arms Export Control Act, 22 U.S.C. 2778, and the Export Administration Act of 1979, 50 U.S.C.App. 2410." 846 F.2d at 594. The district court found the warrant overbroad and suppressed all of the twenty boxes of business records seized by the government.

The Tenth Circuit readily affirmed, explaining that the warrant purported to contain only two limitations:

> First, the documents to be seized had to fall within a long list of business records typical of the documents kept by an export company. Second, those documents had to relate to "the purchase, sale and illegal exportation of materials in violation of the" federal export laws. In this context—the search of the offices of an export company—these limitations provide no limitation at all. The warrant authorizes, and the customs agents conducted, a general search of the … offices.

846 F.2d at 600-01. Here, the list of items gives the appearance, at first glance, of a limitation but the terms of the warrant make clear that it is not, leaving only the unadorned statutory references to serve as any sort of limitation. Those statutory references, however, are themselves even broader than the reference to the Arms Export Control Act and Export Administration Act found insufficient in *Leary*. The Warrants here broadly invoke conspiracy, mail fraud, wire fraud, and obstruction of justice, among others. Because they contain no meaningful limitations, all seven of the *Lustyik* search warrants are facially overbroad and any evidence seized as a result should be suppressed.

IV. The 2012 and 2013 Searches Were Overbroad General Searches

Even if the 2012 and 2013 warrants were not fatally tainted and were themselves not facially invalid or subject to some interpretation that would render them constitutionally reasonable, the seizures actually performed by the government under those warrants in fact were unconstitutional general searches. Subject only to a minimal filter for privileged materials, the government seized (and has produced to the defense as discovery) essentially the entire content of the "searched" media and email accounts.

Courts and commentators have wrestled with how best to balance privacy interests and legitimate law-enforcement concerns in the context of computer searches. One approach would require law-enforcement officials to specify a search protocol *ex ante* and to use, whenever possible, "key word searches ... to distinguish files that fall within the scope of a warrant from files that fall outside the scope of the warrant." Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75, 108 (1994). Another would require the creation of "firewalls" to prevent investigators and prosecutors from obtaining the results of a computer search until documents within the scope of the warrant had been segregated by a third party. The Ninth Circuit recently endorsed variants of both procedures, among others, to minimize the intrusiveness of computer searches while cautioning that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010).

The Tenth Circuit, in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), addressed the particularity requirement as it relates to the search of computer files. In *Carey*, the government obtained a warrant to search two computers owned by the defendant for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the

sale and distribution of controlled substances." *Id.* at 1270. After finding no files "related to drugs," the officers continued to explore various files on the computers and ultimately stumbled upon a JPG file containing child pornography and proceeded to search widely for other images containing child pornography, all without ever obtaining a warrant to search for or seize such materials. *Id.* at 1271.

The defendant moved to suppress the computer files, but the district court denied the motion. The Tenth Circuit reversed, holding that the opening and searching of files not pertaining to the sale or distribution of controlled substances constituted "an unconstitutional general search." 172 F.3d at 1276. The court explained that because computers often contain "intermingled documents" (*i.e.*, documents containing both relevant and irrelevant information), "law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant." *Id.* at 1275. "The underlying premise in *Carey* is that officers conducting searches (and the magistrates issuing warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive. Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer. *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001).

Accordingly, "when officers come across relevant computer files intermingled with irrelevant computer files, they 'may seal or hold' the computer pending 'approval by a magistrate of the conditions and limitations on a further search' of the computer." *Id.* at 986 (quoting *Carey*, 172 F.3d at 1275). What they may not do though is engage in a general rummaging through the entire contents of the entirety of the data. "Officers must be clear as to

what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant." *Walser*, 275 F.3d at 986. While the Tenth Circuit has declined to require that the search warrant itself structure the mechanics of the search in advance, it has made clear that "the search method must be tailored to meet allowed ends" and the search protocol must be structured so as to respect legitimate rights to privacy. *See Burgess*, 576 F.3d at 1094. The Fourth Amendment "surely allows courts to assess the propriety of the government's search methods (the *how*) *ex post* in light of the specific circumstances of each case." *United States v. Christie*, --- F.3d ----, 2013 WL 2477252, at *7 (10th Cir. 2013).

The discovery does not provide a clear or complete picture as to exactly what the government did in all respects with respect to its searches of and seizures from the material obtained for review under the seven warrants here. Are hearing is necessary to determine the precise methodology, if any, employed by the government but the discovery does make some things evident. First, it appears that the government continued the practice from the *Young* case of allowing NTI to peruse the email accounts in their entirety subject to no particular rules or procedure, just to find whatever might be interesting. As reflected by the emails attached as Exhibit U, in January 2013 Ms. Gray and NTI were still perusing Mr. Taylor's email and finding emails and documents from June 2012. Those emails post-dated the December 2011 warrants (and the June 13, 2012 AOL Warrant as well), so she only could have been foraging through them if the results of the September 7, 2012 AOL Warrant were also relayed to her. In any event, the emails seized and distributed to the investigators and prosecutors were beyond the scope of any of the multiple warrants obtained in both cases as they have nothing to do with *either* the investigation of the 2007 procurement activities in connection with the Army contract in Afghanistan *or* Mr. Lustyik or Mr. Thaler, but a completely unrelated business opportunity

AISC was exploring. As such, these emails are only further proof of the government's blatant disregard for even the notion that there might be a limit on their rummaging. They essentially used staggered search warrants to keep general tabs on anything and everything Mr. Taylor or AISC were doing, exactly what the Constitution abhors.

Second, the *Lustyik* prosecutors themselves were given full access at least to the seized email accounts to troll through as they desired. They were not particularly subtle about it either. In a meeting with the government shortly after the Indictment, Kevin Driscoll casually commented to defense counsel that he "had been reading email correspondence between Mr. Taylor and his son" and stated that he had seen that his son was seeking advice about an investment opportunity. (Exh. V, Skordas Declaration ¶ 4-5.) Mr. Driscoll joked that he "thought he might have come across an insider trading case and another indictment against Mr. Taylor and his son" but that, "fortunately" for them, Mr. Taylor had advised his son not to make the investment. (*Id.* ¶¶ 6-7.)

Third, the government has essentially produced to the defense the entirety of the contents of the email accounts seized, amounting to more than 100,000 pages of emails (*see, supra*, footnote 2). These massive files contain all manner of personal emails, emails about entirely unrelated business matters, and assorted spam and advertisements have nothing whatsoever to do with anything remotely relevant to this case. An illustrative collection of examples is attached as Exhibit W, but the instances of this are countless.

The government also appears to have extracted wholesale the entire content of the two cell phones, including data regarding all incoming and outgoing calls (not just calls to/from Mr. Lustyik or Mr. Thaler), the complete substance of any SMS or text messages on the device (all

the way down to a text message wishing his wife "Happy Anniversary! Love you"), all contacts files, and all images. (*See* Under Seal Exhs. W, X, & Y.)

It appears that the government did at least attempt to use some key words or search terms in reviewing the image of the hard drive from Mr. Taylor's laptop (*see* Exh. Z), but the 68-term list used by the government reaches well beyond the scope of any possibly valid construction of the search warrant. It encompasses a host of words and names that were not included on the list contained in Attachment B to the warrant, more than a third of which actually are nowhere mentioned anywhere in the affidavit which accompanied the application (*e.g.*, Iran, BME, Blue meadow energy, *hushmail*, Zak*, *fellah*, *daly*, *cleary*, *newton*, jjnewt*, berlin, *zaye*, *abboud*, Gabby, Erbil, Heyward, Hossam, *Robbie*, *Brandon*, *Paulus*, Diver, Sawzer, *sawyer*). In addition, it contained a number of terms relating to money and finances so common and of general use that they would have captured nearly any business- or finance-related communication or document (*e.g.*, *profit*, Bank, Money, Cash, Loan, Million, Coin, pay, payment). Predictably, the use of an expansive list of search terms, untethered from the warrant or the supporting affidavit and including extremely common words, resulted in the seizure of more than 170,000 Bates-numbered items. (*See* US00171403-00274781, US00998063-01064327, US01069669-01070295.)

V. The Good Faith Exception Does Not Apply

The government may argue that the exclusionary rule should not apply despite the invalidity of the warrants and/or the overbreadth of the searches and seizures conducted thereunder by virtue of the "good faith" exception created in *United States v. Leon*, 468 U.S. 897 (1984). In *Leon*, the Supreme Court modified the Fourth Amendment exclusionary rule to provide that evidence seized under a warrant later found to be invalid may be admissible if the

executing officers acted in good faith and in reasonable reliance on the warrant. *United States v. Medlin*, 798 F.2d 407, 409 (10th Cir. 1986). The *Leon* Court applied the "good faith" exception to admit the evidence from a search warrant subsequently invalidated by a lack of probable cause. In *Massachusetts v. Sheppard*, 468 U.S. 981, 988 (1984) the Court held that the same exception could also be applied to warrants that violate the fourth amendment's particularity requirement.

In determining whether the exception should be applied, the "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n. 23. To answer this "objectively ascertainable question," we are to consider "all of the circumstances," *id.*, and assume that the executing "officers have a reasonable knowledge of what the law prohibits." *Id.* at 919 n. 20.

Of course, *Leon* does not mean that evidence obtained under an invalid warrant should never be suppressed. Rather, the Supreme Court simply held that the use of the exclusionary rule should be confined to those cases in which its purposes would be served, *i.e.*, in circumstances under which it would deter police misconduct. The Court identified certain circumstances where suppression remains an appropriate remedy, including where the warrant is "so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923 (citations omitted).

The Tenth Circuit previously has held that the government may not rely on the "good faith" exception in cases where "the warrant [is] so facially deficient in its description of the items to be seized that the executing officers could not reasonably rely on it." *Leary*, 846 F.2d at

609. In *Leary*, the court found the good faith exception inapplicable based on the expansive scope of the warrant evident from its face and the government's conduct and the circumstances of the search, which involved no effort to limit the seizures made under the warrant. *Id.* at 609-10. The Tenth Circuit held that the general search in that case "exemplifies the very type of official conduct the exclusionary rule is intended to deter." *Id.* at 610 (quoting *United States v. Owens*, 782 F.2d 146, 152 (10th Cir. 1986)).

By contrast, the Tenth Circuit has permitted application of the good faith exception in cases where despite the invalidity of the warrant, the officers conducting the search nevertheless acted as if they were subject to limitations and employed a search methodology limited to uncovering the type of items for which probable cause had been established and seized only evidence of that nature. *See, e.g.*, *Riccardi*, 405 F.3d at 863-64 (finding good faith exception applied where, *inter alia*, "the investigating officers carefully limited their search to files relevant to the investigation, and within the scope of the search as described by the affidavit" and "temporarily suspended their search to examine the terms of the warrant and to obtain legal counsel" and "resumed the search only after receiving assurance from the prosecutor that they were acting lawfully"). Here though, the government does not appear to have employed any particular methodology at all in searching the massive amounts of electronic data, and what methodology it may have employed in searching the image of the laptop was so flawed and over-inclusive as to render it meaningless as any sort of limitation, must less a limitation tied in any way to the warrant under which the search supposedly was conducted.

CONCLUSION

For the foregoing reasons and those set forth in the Motion to Suppress filed in the *Young* case, Defendant Taylor respectfully requests that the Court suppress all evidence seized pursuant

to the December 2011 search warrants directed at AISC and Mr. Taylor's email and computers. Mr. Taylor further moves to suppress all evidence obtained by the government as a result of the search warrants obtained in connection with this case since May 2012 because those warrants were obtained through use of fruits of the unconstitutional searches in the *Young* case. In addition, if they are not suppressed in any event as fruit of the poisonous tree, we request that any and all evidence obtained as a result of the June 13, 2012, August 2, 2012, September 7, 2012, September 21, 2012, October 18, 2012, and January 15, 2013 search warrants directed specifically at email accounts and property allegedly associated with Mr. Taylor be suppressed because those warrants are facially unconstitutional general warrants.

In the alternative, the defense requests that the Court schedule a hearing regarding the government's use of the emails unlawfully-obtained in the *Young* case and the process, manner, and methods by which the government conducted their searches of and seizures from these electronic materials and any fact-based defense or exception the government may contend applies. The defense requests that the Court order the government to produce the following witnesses to testify at the hearing regarding these matters:

1. Special Agent Keith Darnell, Defense Criminal Investigative Services;
2. Special Agent James P. Donahue, Department of Homeland Security;
3. Jessica Gray, NTI Law Enforcement Investigative Support Services;
4. Special Agent Shaun Helt, Department of Homeland Security;
5. Special Agent Thomas M. Hopkins, Department of Justice, Office of the Inspector General;
6. Special Agent Kerwin John, Department of Justice, Office of the Inspector General;

7. Special Agent Harry A. Lidsky, Department of Justice, Office of the Inspector General;
8. Sandra Slowik, Department of Justice, Office of the Inspector General; and
9. Special Agent Alicia Vazquez, Department of Justice, Office of the Inspector General

In addition, the defense further requests that the Court order both the government and NTI Law Enforcement Investigative Support Services to produce, prior to the hearing, any and all documents (including but not limited to emails) relating to the searches of and seizures from the email files and forensic images provided to NTI.

Dated: August 9, 2013

Respectfully Submitted,

/s/Tillman J. Finley

Daniel Marino (admitted *pro hac vice*)
Tillman J. Finley (admitted *pro hac vice*)
MARINO LAW PLLC
910 17th Street, N.W., Suite 800
Washington, DC 20006
Telephone: (202) 223-8888
Facsimile: (877) 239-2146

REBECCA HYDE SKORDAS (6409)
Skordas, Caston, & Hyde
341 S. Main Street, Suite 303
Salt Lake City UT 84111-2707
Telephone: (801) 531-74444
Facsimile: (801) 531-8885

Attorneys for Michael Taylor